Amendments to the Claims

Claim 1 (currently amended): A computer program product for efficiently generating pseudo-random bits, the computer program product embodied on one or more computer readable media and comprising:

computer-readable program code means for providing an input value; [[and]]

computer-readable program code means for generating an output sequence of pseudo-random bits using the provided input value as input to a 1-way function, wherein a length in bits, C, of the input value is substantially shorter than a length in bits, N, of the generated output sequence; and

computer-readable program code means for using C selected bits of the generated output sequence as the provided input value for a next iteration of the computer-readable program code means for generating while using all N - C remaining bits of the generated output sequence as pseudo-random output bits, until a desired number of pseudo-random output bits have been generated.

Claim 2 (original): The computer program product according to Claim 1, wherein the 1-way function is based upon an assumption known as "the discrete logarithm with short exponent" assumption.

Claim 3 (original): The computer program product according to Claim 1, wherein the 1-way function is modular exponentiation modulo a safe prime number.

Claim 4 (currently amended): The computer program product according to Claim 3, wherein the input value is used as an exponent of the modular exponentiation.

Claim 5 (original): The computer program product according to Claim 3, wherein a base of the modular exponentiation is a fixed generator value.

Claim 6 (original): The computer program product according to Claim 4, wherein the length of the input value is 160 bits and a length of the safe prime number is 1024 bits.

Claim 7 (original): The computer program product according to Claim 1, wherein the length of the input value is at least 160 bits and the length of the generated output sequence is at least 1024 bits.

Claim 8 (canceled)

Claim 9 (currently amended): The computer program product according to Claim [[8]] 1, wherein the N - C remaining bits are concatenated to pseudo-random output bits previously generated by the computer-readable program code means for generating ~~further comprising:~~

~~computer-readable program code means for concatenating bits of the generated next sequential output sequence which are not selected by the computer-readable program code means for selecting to the generated output sequence to form a longer output sequence of pseudo-random bits.~~

Claim 10 (currently amended): The computer program product according to Claim [[8]] 1, wherein the N - C remaining bits are selected from the N bits of the generated output sequence as ~~computer-readable program code means for selecting the subset of bits comprises selecting~~ a contiguous group of bits.

Claim 11 (currently amended): The computer program product according to Claim [[8]] 1, wherein the N - C remaining bits are selected from the N bits of the generated output sequence as ~~computer-readable program code means for selecting the subset of bits comprises selecting~~ a non-contiguous group of bits.

Claim 12 (currently amended): The computer program product according to Claim [[8]] 1, further comprising computer-readable program code means for using the desired number of generated pseudo-random bits ~~longer output sequence~~ as input to an encryption operation.

Claim 13 (currently amended): A system for efficiently generating pseudo-random bits in a computing environment, comprising:

means for providing an input value; [[and]]

means for generating an output sequence of pseudo-random bits using the provided input value as input to a 1-way function, wherein a length in bits, C, of the input value is substantially shorter than a length in bits, N, of the generated output sequence; and

means for using C selected bits of the generated output sequence as the provided input

value for a next iteration of the means for generating while using all N - C remaining bits of the generated output sequence as pseudo-random output bits, until a desired number of pseudo-random output bits have been generated.

Claim 14 (original): The system according to Claim 13, wherein the 1-way function is based upon an assumption known as "the discrete logarithm with short exponent" assumption.

Claim 15 (original): The system according to Claim 13, wherein the 1-way function is modular exponentiation modulo a safe prime number.

Claim 16 (currently amended): The system according to Claim 15, wherein the input value is used as an exponent of the modular exponentiation.

Claim 17 (original): The system according to Claim 15, wherein a base of the modular exponentiation is a fixed generator value.

Claim 18 (original): The system according to Claim 16, wherein the length of the input value is 160 bits and a length of the safe prime number is 1024 bits.

Claim 19 (original): The system according to Claim 13, wherein the length of the input value is at least 160 bits and the length of the generated output sequence is at least 1024 bits.

Claim 20 (canceled)

Claim 21 (currently amended): The system according to Claim [[20]] 13, wherein the N - C remaining bits are concatenated to pseudo-random output bits previously generated by the means for generating ~~further comprising:~~

~~means for concatenating bits of the generated next sequential output sequence which are not selected by the means for selecting to the generated output sequence to form a longer output sequence of pseudo-random bits.~~

Claim 22 (currently amended): The system according to Claim[[20]] 13, wherein the N - C remaining bits are selected from the N bits of the generated output sequence as ~~means for selecting the subset of bits comprises selecting~~ a contiguous group of bits.

Claim 23 (currently amended): The system according to Claim [[20]] 13, wherein the N - C remaining bits are selected from the N bits of the generated output sequence as ~~means for selecting the subset of bits comprises selecting~~ a non-contiguous group of bits.

Claim 24 (currently amended): The system according to Claim [[20]] 13, further comprising means for using the desired number of generated pseudo-random output bits ~~longer output sequence~~ as input to an encryption operation.

Claim 25 (currently amended): A method for efficiently generating pseudo-random bits,

comprising the steps of:

providing an input value; [[and]]

generating an output sequence of pseudo-random bits using the provided input value as input to a 1-way function, wherein a length in bits, C, of the input value is substantially shorter than a length in bits, N, of the generated output sequence; and

using C selected bits of the generated output sequence as the provided input value for a next iteration of the generating step while using all N - C remaining bits of the generated output sequence as pseudo-random output bits, until a desired number of pseudo-random output bits have been generated.

Claim 26 (original): The method according to Claim 25, wherein the 1-way function is based upon an assumption known as "the discrete logarithm with short exponent" assumption.

Claim 27 (original): The method according to Claim 25, wherein the 1-way function is modular exponentiation modulo a safe prime number.

Claim 28 (currently amended): The method according to Claim 27, wherein the input value is used as an exponent of the modular exponentiation.

Claim 29 (original): The method according to Claim 27, wherein a base of the modular exponentiation is a fixed generator value.

Claim 30 (original): The method according to Claim 28, wherein the length of the input value is at least 160 bits and a length of the safe prime number is at least 1024 bits.

Claim 31 (original): The method according to Claim 25, wherein the length of the input value is 160 bits and the length of the generated output sequence is 1024 bits.

Claim 32 (original): The method according to Claim 25, wherein the length of the input value is at least 160 bits and the length of the generated output sequence is at least 1024 bits.

Claim 33 (canceled)

Claim 34 (currently amended): The method according to Claim [[33]] 25, wherein the N - C remaining bits are concatenated to pseudo-random output bits previously generated by the generating step ~~further comprising the step of concatenating bits of the generated next sequential output sequence which are not selected by the selecting step to the generated output sequence to form a longer output sequence of pseudo-random bits~~.

Claim 35 (currently amended): The method according to Claim [[33]] 25, wherein the N - C remaining bits are selected from the N bits of the generated output sequence as ~~step of selecting the subset of bits comprises selecting~~ a contiguous group of bits.

Claim 36 (currently amended): The method according to Claim [[33]] 25, wherein the N - C

remaining bits are selected from the N bits of the generated output sequence as ~~step of selecting the subset of bits comprises selecting~~ a non-contiguous group of bits.

Claim 37 (currently amended): The method according to Claim [[33]] 25, further comprising the step of using the desired number of generated pseudo-random output bits ~~longer output sequence~~ as input to an encryption operation.

Claim 38 (canceled)

Claim 39 (currently amended): An encryption system, comprising:

means for providing an input value;

means for generating an output sequence of pseudo-random bits using the provided input value as input to a 1-way function, wherein a length in bits, C, of the input value is substantially shorter than a length in bits, N, of the generated output sequence;

means for using C selected bits of the generated output sequence as the provided input value for a next iteration of the means for generating while using all N - C remaining bits of the generated output sequence as pseudo-random output bits, until a desired number of pseudo-random output bits have been generated; and

means for using the desired number of generated pseudo-random bits ~~of the generated output sequence~~ as input to an encryption operation.

Claim 40 (original): The encryption system according to Claim 39, wherein the 1-way function

is based upon an assumption known as "the discrete logarithm with short exponent" assumption.

Claim 41 (original): The encryption system according to Claim 39, wherein the 1-way function is modular exponentiation modulo a safe prime number.

Claim 42 (currently amended): The encryption system according to Claim 41, wherein the input value is used as an exponent of the modular exponentiation.

Claim 43 (original): The encryption system according to Claim 41, wherein a base of the modular exponentiation is a fixed generator value.

Claim 44 (original): The encryption system according to Claim 42, wherein the length of the input value is 160 bits and a length of the safe prime number is 1024 bits.

Claim 45 (original): The encryption system according to Claim 39, wherein the length of the input value is 160 bits and the length of the generated output sequence is 1024 bits.

Claim 46 (canceled)

Claim 47 (currently amended): The encryption system according to Claim 46, wherein the N - C remaining bits are concatenated to pseudo-random output bits previously generated by the means for generating ~~further comprising:~~

means for concatenating bits of the generated next sequential output sequence which are not selected by the means for selecting to the generated output sequence to form a longer output sequence of pseudo-random bits; and

wherein the means for using bits of the generated output sequence as input to the encryption operation further comprises means for using the longer output sequence as the input to the encryption operation.